The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

Subject:
Vulnerabilities in the BlackBerry Enterprise Server (KB19860)

Overview:
Multiple security vulnerabilities exist in the PDF distiller of some released versions of the BlackBerry Attachment Service component of the BlackBerry Enterprise Server. These vulnerabilities could enable a malicious individual to send an email message containing a specially crafted PDF file, which when opened for viewing on a BlackBerry smartphone that is associated with a user account on a BlackBerry Enterprise Server, could cause memory corruption and possibly lead to a Denial of Service (DoS) condition or arbitrary code execution on the computer that hosts the BlackBerry Attachment Service component of that BlackBerry Enterprise Server.

Risk:
High

Affected Products:
BlackBerry Enterprise Server software version 5.0.0 running on Microsoft® Windows® version 2003 or 2008
BlackBerry Enterprise Server software version 5.0.0 running on Microsoft Windows version 2000
BlackBerry Enterprise Server software version 4.1 Service Pack 3 (4.1.3) through 4.1 Service Pack 7 (4.1.7)
BlackBerry Professional Software 4.1 Service Pack 4 (4.1.4)

Non-Affected Products:
BlackBerry Enterprise Server version 4.1.2 and earlier
BlackBerry® Device Software on all BlackBerry smartphones
BlackBerry® Desktop Software

Solution:
RIM has issued the following releases and interim security software updates that resolve these vulnerabilities in affected versions of the BlackBerry Enterprise Server and BlackBerry Professional Software.

For BlackBerry Enterprise Server version 5.0 for Microsoft Exchange and IBM Lotus Domino
Visit http://www.blackberry.com/go/serverdownloads to upgrade to BlackBerry Enterprise Server Version 5.0.1 or later, or obtain Interim Security Update 3 for BlackBerry Enterprise Server software version 5.0.0.
For BlackBerry Enterprise Server version 4.1.7 for Microsoft Exchange and IBM Lotus Domino

Visit http://www.blackberry.com/go/serverdownloads to obtain Interim Security Update 1 for BlackBerry Enterprise Server software version 4.1.7.

For BlackBerry Enterprise Server version 4.1.6 for Microsoft Exchange and IBM Lotus Domino

Visit http://www.blackberry.com/go/serverdownloads to upgrade to BlackBerry Enterprise Server Version 4.1.6 MR8 or later.

For BlackBerry Enterprise Server version 4.1.6 for Novell GroupWise

Visit http://www.blackberry.com/go/serverdownloads to upgrade to BlackBerry Enterprise Server Version 4.1.6 MR6 or later.

For BlackBerry Enterprise Server version 4.1.4

Visit http://www.blackberry.com/go/serverdownloads to upgrade to BlackBerry Enterprise Server Version 4.1.6 MR8 or later, or obtain Interim Security Update 5 for BlackBerry Enterprise Server software version 4.1.4.

For BlackBerry Professional Software

Visit http://na.blackberry.com/eng/support/downloads/#tab_professional to obtain Interim Security Update 5 for affected BlackBerry Professional Software versions.

Workaround:

Note: As a mobile device best practice, RIM recommends that BlackBerry smartphone users open attachments from trusted sources only.

Prevent the BlackBerry Attachment Service from processing PDF files in a BlackBerry Enterprise Server environment

The administrator can prevent the BlackBerry Attachment Service from processing PDF files by editing the list of file format extensions that the BlackBerry Attachment Service opens, and then preventing the PDF attachment distiller from running on the BlackBerry Attachment Service.

To remove the PDF file extension from the list of supported file format extensions, complete the following actions:

For BlackBerry Enterprise Server versions earlier than 5.0, and BlackBerry Professional Software

From the Windows Desktop, open the BlackBerry Server Configuration tool.
Click the Attachment Server tab.
In the Format Extensions field, delete pdf: from the colon–delimited list of extensions.
Click Apply.
Click OK.

For BlackBerry Enterprise Server version 5.0 or later

In the BlackBerry Administration Service, on the Servers and components menu, expand BlackBerry Solution topology > BlackBerry Domain > Component view > Attachment > Connector.
Click the BlackBerry Attachment Connector instance that is associated with the BlackBerry Attachment Service that you want to change.
In the Suport Attachment Server instances tab, click Edit instance.
Click the Edit icon.
Click the Delete icon for the PDF extension.
Click Save all.

Until the administrator prevents the PDF attachment distiller from running, the BlackBerry Attachment Service still detects a PDF file with a renamed extension (in other words, its extension is not .pdf) and attempts to process the file automatically. To prevent the PDF attachment distiller from running, complete the following actions:

For BlackBerry Enterprise Server versions earlier than 5.0, and BlackBerry Professional Software

On the Windows Desktop, open the BlackBerry Server Configuration tool.
Click the Attachment Server tab.
In the Configuration Option drop-down list, select Attachment Server.
In the Distiller Settings section, next to the distiller name Adobe PDF, clear the check box in the Enabled column.
Click Apply.
Click OK.
On the Windows Desktop, in Administrative Tools, open Services.
Right-click BlackBerry Attachment Service and click Stop.
Right-click BlackBerry Attachment Service and click Start.
Close Services.

For BlackBerry Enterprise Server version 5.0 or later

In the BlackBerry Administration Service, on the Servers and components menu, expand BlackBerry Solution topology > BlackBerry Domain > Component view > Attachment > Server.
Click the instance that you want to change.
Click Edit instance.
In the Distiller section, in the Allowed column, specify which distillers are supported for the instance.
Click Save.
Restart the BlackBerry Attachment Service.

For all versions

In Microsoft Exchange and Novell GroupWise environments , complete the following additional steps:
On the Windows Desktop, in Administrative Tools, open Services.
Right-click BlackBerry Dispatcher and click Stop.
Right-click BlackBerry Dispatcher and click Start.
Close Services.

Note: Restarting BlackBerry Enterprise Server services might delay message delivery to BlackBerry devices. For more information, see KB04789.

In IBM Lotus Domino environments, complete the following additional steps:

For BlackBerry Enterprise Server versions earlier than 5.0, and BlackBerry Professional Software

Open the Lotus Domino Administrator.
Click the Server tab.
Click the Status tab.

Click Server Console.
In the Domino Command field, type tell BES quit and press ENTER.
In the Domino Command field, type load BES and press ENTER.
Close the Lotus Domino Administrator.

For BlackBerry Enterprise Server version 5.0 or later

Note: The administrator should not use the IBM Lotus Domino console to stop and start the BlackBerry Messaging Agent. If the administrator uses the IBM Lotus Domino console, the BlackBerry Messaging Agent libraries might not load properly and, if the administrator configures high availability, the BlackBerry Messaging Agent might not start correctly as the primary or standby instance.

Stop and start the BlackBerry Controller service and BlackBerry Dispatcher service in the Windows Services, or stop and start the BlackBerry Enterprise Server in the BlackBerry Administration Service.

REFERENCES:

RIM
http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB19860